PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 11/00

A1

(11) International Publication Number: WO 97/37305

(43) International Publication Date: 9 October 1997 (09.10.97)

(21) International Application Number: PCT/US97/04905

(22) International Filing Date: 27 March 1997 (27.03.97)

(30) Priority Data:
08/626,221 29 March 1996 (29.03.96) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, P.O. Box 58119, Santa Clara, CA 95052-8119 (US).

(72) Inventors: TRAW, C., Brendan, S.; 5302 S.E. Baseline Road #220, Hillsboro, OR 97123 (US). HANNAH, Eric, C.; 3046 Strawberry Hill, Pebble Beach, CA 93953 (US). HAUCK, Jerrold, V.; 39283 Marbella Terraza, Fremont, CA 94538 (US). COULSON, Richard, L.; 17454 N.W. Gilbert Lane, Portland, OR 97229 (US). HOSLER, Brad, W.; 11351 N.W. East Road, Portland, OR 97229 (US).

(74) Agents: MURRAY, William, H. et al.; Suite 3600, 1600 Market Street, Philadelphia, PA 19103-4252 (US).

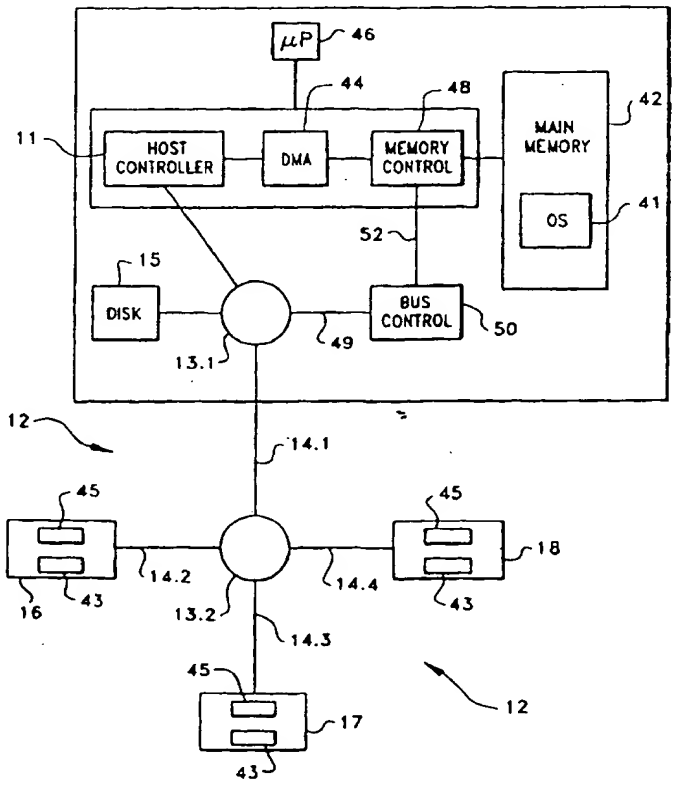
(81) Designated States: CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: COMPUTER SYSTEM SECURITY

(57) Abstract

Security from an unwanted intrusion into a computer system (12) is provided by coupling a host component (10) with a peripheral component (16-18) using a high-speed serial bus (14.1-14.4) having a high-speed physical layer and using features of the bus (14.1-14.4) to implement the security. In an embodiment, the high-speed serial bus (14.1-14.4) has a secondary bus layer that is used to implement a number of the security features of the invention.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

COMPUTER SYSTEM SECURITY

CROSS-REFERENCES TO RELATED APPLICATIONS

This non-provisional U.S. national application, filed under 35 U.S.C. §111(a) claims, under 35 U.S.C. §119(e)(1), the benefit of the filing date of provisional U.S. applications nos. 60/006,431, filed under 35 U.S.C. §111(b) on November 10, 1995; 60/011,320, filed under 35 U.S.C. §111(b) on February 8, 1996; and (to be provided), filed under 35 U.S.C. §111(b) on March 8, 1996 as attorney docket no. 366431-122P3, the teachings of all three being incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of computer system security for preventing unwanted intrusion into a computer system.

2. Background of the Invention

The vast amount of data and information stored in and processed by computers makes them obvious targets for corporate spies and other information thieves. Unfortunately, computers generally are susceptible to security breaches. An ability of a bus coupling a host computer to one or more peripherals to use a direct memory access (DMA) engine to directly read from and write to the host computer's physical memory locations exacerbates the problem. For example, a rogue device can be tapped into the network and can use the DMA engine to obtain massive amounts of data from the host and its peripherals. A bus with this ability to use a host DMA engine is described in U.S. Provisional Applications Serial Nos. 60/006,431; 60/011,320; and attorney docket no. 366431-122P3, filed on November 10, 1995, February 8, 1996, and March 8, 1996, respectively. Since peripherals attached to such a bus may be several meters away from the host computer, an unwanted attachment of a rogue device to the bus which could monitor data traffic on the bus and directly access host memory could go unnoticed by legitimate system users.

Conventionally, an addition of security features to a modern, high-performance computer system necessitated incurring substantial costs, especially in order to avoid causing diminished system performance. There is a need, therefore, for a reliable, low-cost security

system to prevent unwanted intrusions into a computer system. Optimally, the system should not affect system performance.

SUMMARY OF THE INVENTION

Security from an unwanted intrusion into a computer system is provided by coupling a host component with a peripheral component using a high-speed serial bus having a high-speed physical layer and using features of the bus to implement the security.

BRIEF DESCRIPTION OF THE DRAWINGS

The following detailed description will be more fully understood with reference to the accompanying drawings in which:

Fig. 1 is a block diagram of a system of the invention using a high-speed serial bus for providing security;

Fig. 2 is a schematic of a high-speed serial bus cable;

Fig. 3 is a schematic view of the wiring of the cable shown in Fig. 2.

Fig. 4 is a flow chart of the operation of an embodiment of the invention;

Fig. 5 is a flow chart of the operation of another embodiment of the invention; and

Fig. 6 is a flow chart of yet another embodiment of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

A topology of a system embodying the invention is shown in Fig. 1. Host computer 10 includes host controller 11, which provides an interface to bus hub 13.1. Host controller 11 governs data movement between host 10 and peripherals 16-18 and provides an interface to the memory system of host 10, such as DMA engine 44, memory controller 48 and memory 42. Host controller 11 is coupled to DMA engine 44, which is coupled to memory controller 48. In an embodiment, host controller 11, DMA engine 44 and memory controller 48 are part of a single integrated circuit.

The high-speed physical layer or links of bus system 12, to be described below, can communicate with DMA engine 44 to directly access memory 42, for example through memory controller 48. The direct memory accessing capability of bus system 12 contributes

to the very low latency of the bus system. Peripherals on bus system 12, such as peripherals 16-18 are permitted real-time, direct access to host memory 42 using DMA engine 44.

Bus system 12 includes hub 13.1 located within the confines of host computer 10. One or more mass storage devices such as disk drive 15 is coupled to hub 13.1. Bus cable 14.1 couples internal hub 13.1 to external hub 13.2 onto which a plurality of peripherals can be coupled. Various peripherals 16-18 can be coupled to hub 13.2 by bus cables 14.2, 14.3 and 14.4. For the purposes of this disclosure, the high-speed bus and bus system 12 means any of cables 14.1-14.4 and hubs 13.1 and 13.2. Peripherals which can be coupled to hubs 13.1 or 13.2 include, for example, printers, scanners, cameras, disk drives, network interfaces, etc. As should be apparent to one of ordinary skill, coupled peripherals can be a substantial distance from host 10, especially when using multiple linked hubs 13.x. Furthermore, the high-speed links of bus cables 14.1 - 14.4 and hubs 13.1 and 13.2 use DMA engine 44 to allow peripherals 16-18 to directly access host computer memory 42. Although this latter feature of the bus helps provide it with the qualities of low latency and high bandwidth, it also makes host memory susceptible to unauthorized access by rogue devices coupled to any of buses 14.1 - 14.4 or hubs 13.1 and 13.2. The invention protects the security of host computer 10 to help prevent a hacker from directly accessing main memory 42 using DMA engine 44, through memory controller 48.

A schematic view of a bus cable is shown in Fig. 2. Fig. 2 shows, for example, bus cable 14.2 linking peripheral 16 to external hub 13.2, but it should be understood that Fig. 2. also can represent any of bus cables 14.1-14.4 and hubs 13.1 and 13.2. Bus cable 14.2 has a pair of opposing, unidirectional, high speed, shielded, twisted pairs defining high-speed physical layers or links 21 and 22, linking transceiver pairs 23 and 24. Transceivers 23 and 24 are AC coupled via shielded links 21 and 22 with 100 ohm differential impedance. Transceiver 23 has driver 25 and receiver 26. Transceiver 24 has driver 27 and receiver 28. Bus cable 14.2 also includes a secondary bus component 34, such as a Universal Serial Bus (USB), having link 28 which comprises a bidirectional pair coupling transceiver 29 with transceiver 30. USB is well known to those having skill in the art and a technical specification on the bus can be found on the World Wide Web at Uniform Resource Locator (URL) address http://www.teleport.com/~usb/. The invention makes substantial use of the secondary bus component in all of bus cables 14.1 - 14.4 and hubs 13.1 and 13.2 as service layers for implementing many security features of the invention, as will be more fully described below.

The secondary link, such as a USB link, is available for implementing the security features because unlike the high-speed links of bus cables 14.1-14.4 and hubs 13.1 and 13.2, the secondary links do not have DMA engine access. No danger exists that a rogue device can access memory through the secondary links. Access to memory through the secondary links is controlled entirely, for example, by computer 10, for example by operating system 41 and processor 46, and thus the secondary links are inherently trusted by computer 10. No device can access host memory 42 through the secondary links without processor 46 and operating system 41 knowing about it. A peripheral using an active high-speed link of the bus system of the invention may directly access host memory 42, however, using DMA engine 44, without knowledge by processor 46 or operating system 41. It should be understood by a person of ordinary skill that operation of processor 46 and operating system 41 are mutually dependent and reference to one necessarily incorporates reference to the other.

The secondary links of bus cables 14.1-14.4 and hubs 13.1 and 13.2 are split-off from the high-speed links inside of computer 10. For example, a secondary lead 49 provides a secondary bus path to secondary bus controller 50. In an embodiment of the invention, secondary bus controller 50 is a USB bus controller known to those having skill in the art. Secondary bus controller 50 is coupled to memory controller 48 through an input/output (I/O) bus 52, such as a peripheral control interface (PCI) bus inside computer 10.

Fig. 3 is a more detailed view of high-speed links 21 and 22 and secondary link 28 of bus cable 14.2. High-speed links 21 and 22 are twisted pairs having internal shielding 31. Links 21 and 22 are unidirectional, but combine to provide full-duplex communications. Secondary link 28 is a bi-directional, twisted pair path. All of links 21, 22, and 28 are shielded by shield 39. Voltage supply 32 and ground wires 33 also are associated with the secondary component 34 of bus cable 14.2.

The invention uses the secondary links in one or more of the high-speed bus cables 14.1-14.4 to provide the security features of the invention. For example, one method of providing security is to prevent use of a high-speed link, such as links 21 and 22 of bus cable 14.2, for example by disabling (or not enabling) transceivers 23 and 24 until the identity of a peripheral component, such as printer 16, is verified through the secondary links. Preferably, this is done at system initialization (step 61 at Fig. 4). For example, processor 46 and software in computer node 10, for example operating system 41, can attempt to identify the peripheral, such as peripheral 16, for example by checking through the secondary links for

expected switch settings in switch 43 (step 62). A signal delivered to peripheral 16 from computer node 10 will be altered in a definable manner according to the switch settings, returned over the secondary links (step 63) and interpreted by processor 46 and operating system 41 in computer node 10 as a valid or invalid verification of the identity of peripheral 16 (step 63). In an alternative embodiment, an active component in a peripheral, such as peripheral 16, could transmit an expected message back to computer node 10 through the secondary links in response to a query or challenge received through the secondary links (step 64). Various authentication protocols, which are known to those having skill in the art, may be used by host 10 and a peripheral, such as peripheral 16, in the challenge and response transmissions. In any event, if the peripheral, such as peripheral 16 is affirmatively identified (step 64), operating system 41 in computer node 10 permits use of high-speed links 21 and 22 (step 65), such as by enabling high-speed transceivers 23 and 24 and use of other high-speed links in the physical data transmission path to peripheral 16. Use of the high-speed links is denied if the peripheral is not identified (step 66).

In another embodiment that uses the secondary links of bus cables 14.1 - 14.4, a writable storage medium, such as storage medium 45, can be installed in a peripheral intended for use with the bus system of the invention. The storage medium can be pre-encoded with a unique signature. In another embodiment, upon initial installation of the peripheral, software, such as operating system 41 resident in memory 42 on host computer 10 writes into storage medium 45 through secondary links the unique identifying code, which will be "remembered" by operating system 41 as the peripheral's dedicated signature. During subsequent system initializations (step 61), the operating system 41 in computer node 10 queries the peripheral through the secondary links (step 62), such as secondary link 28, for the dedicated signature stored in the storage medium 45 (step 63) before permitting use of the high-speed links (step 65), such as before enabling transceivers 23 and 24, for high-speed data transmission over the high-speed links of a bus cable, such as high speed links 21 and 22. Use of the high-speed links is denied to peripherals which fail to exhibit a proper signature to operating system 41 over the secondary links (step 66). Storage medium 45 can be, for example, a flash ROM into which the dedicated signature is stored by operating system 41 in computer node 10. In an embodiment, the high-speed links are enabled automatically, such as by operating system 41, upon recognition of the peripheral.

Another feature of the invention provides a user of computer 10 with an opportunity to manually approve a change in system configuration. For example, a configuration of system 12 can be checked by operating system 41, for example at system initialization (step 71 of Fig. 5), through the secondary links of bus cables 14.1-14.4 and hubs 13.1-13.2, for example by investigating the presence and content of various known registers in peripherals as known by persons having ordinary skill in the art (step 72). In an embodiment of the invention, if a peripheral is found to have been added or removed through responses to the queries received over the secondary bus links (steps 73 and 74), operating system 41 generates a dialog box on a monitor attached to computer 10 (not shown in Fig.1) to notify the user (step 75). Preferably, the user is requested to input instructions in response to the information gathered over the secondary links (step 76). For example, in the event a rogue device has been attached, the user can instruct the system to refrain from activation, such as by not enabling, or disabling, the high-speed transceivers of the high-speed data links of one or more of bus cables 14.1-14.4 and hubs 13.1 -13.2 (step 77). A user also can cause acceptance of the peripheral (step 79), such as by entering the appropriate information including, preferably, a password when confronted with the dialog box generated by operating system 41 (step 78).

Even after a system has been initialized and is running, the invention continues to provide security from unwanted intrusions and attempts to access memory 42. For example, operating system 41, through the secondary links of bus cables 14.1-14.4 and hubs 13.1 and 13.2, continues to monitor the system as it is running for an occurrence of any real-time plug and unplug events i.e., connections or disconnections of a peripheral while the system is running (step 81 of Fig. 6). In an embodiment, any connections or disconnections of a peripheral into hubs 13.1 or 13.2, or along any of bus cables 14.1 - 14.4 are detected by operating system 41 through the secondary links of the bus system (step 82). A user of computer node 10 preferably is notified of the hot plug or unplug, such as through a dialog box as discussed above, and can investigate the occurrence to learn of its nature (step 83). In a preferred embodiment, the dialog box specifies, for example, the location and identity of the hot plug or unplug. An interested user at host computer 10 can investigate the notification to determine whether unauthorized access has occurred or been attempted (step 84). In an embodiment, the user can enter a password allowing a hot-plugged peripheral to join the system (step 85), such as by enabling the relevant high-speed transceivers in any of bus cables 14.1-14.4 and hubs 13.1-13.2 (step 86). Of course, use of the high-speed links for

unauthorized access will be prevented (step 87), either affirmatively or by a simple failure to enter authorization, such as a password, when prompted.

The invention therefore provides a variety of non-exclusive, low-cost and easily implemented security measures which protect a computer system from an unwanted intrusion. These security measures are especially important considering the direct memory accessing capabilities which can be provided using the high speed links of bus cables 14.1-14.4 and hubs 13.1 and 13.2 through DMA engine 44, which could be used for unauthorized accessing of main memory 42.

As described above, processor 46 and operating system 41 substantially control security system functionality, such as by generating and transmitting peripheral device queries, receiving responses thereto and generating graphical user interfaces, such as dialog boxes, pertaining to security issues. It should be understood to a person having ordinary skill that the activities of processor 46 and operating system 41 with respect to implementation of the security features of the invention can be handled by dedicated hardware and software, for example an expanded host controller 11 and special software in a dedicated memory or in memory 42.

The invention is described above with reference to a limited number of bus cables and hubs. It should be understood that the use of additional hubs and cables coupling additional peripherals to host 10 is within the scope of the invention.

The present invention can be embodied in the form of computer-implemented processes and apparatuses for practicing those processes. The present invention also can be embodied in the form of computer program code embodied in tangible media, such as floppy diskettes, CD-ROMs, hard drives, or any other computer-readable storage medium, wherein, when the computer program code is loaded into and executed by a computer, the computer becomes an apparatus for practicing the invention. The present invention can also be embodied in the form of computer program code, for example, whether stored in a storage medium, loaded into and/or executed by a computer, or transmitted over some transmission medium, such as over electrical wiring or cabling, through fiber optics, or via electromagnetic radiation, wherein, when the computer program code is loaded into and executed by a computer, the computer becomes an apparatus for practicing the invention.

When implemented on a general-purpose microprocessor, the computer program code segments configure the microprocessor to create specific logic circuits.

It should be understood that various changes in the details, materials, and arrangements of the parts which have been described and illustrated in order to explain the nature of this invention may be made by those skilled in the art without departing from the principle and scope of the invention as expressed in the following claims.

5

CLAIMS

What we claim is:

1. A method for providing security from an unwanted intrusion into a system, comprising the steps of:

(a) coupling a host with a peripheral using a high-speed serial bus having a high-speed physical layer; and

(b) using features of the bus to implement the security.

2. The method of claim 1, wherein step (b) comprises the step of using a secondary bus within the high-speed serial bus to implement the security.

3. The method of claim 2, wherein the high-speed physical layer and not the secondary bus has direct memory accessing capability.

4. The method of claim 2, wherein step (b) comprises the step of using the secondary bus to query an identity of the peripheral.

5. The method of claim 4, further comprising the step of:

(c) generating an indicator concerning the identity of the peripheral.

6. The method of claim 5, further comprising the steps of:

(d) accepting verification from a user of the identity of the peripheral; and

(e) permitting use of the high-speed physical layer coupling to the peripheral.

7. The method of claim 4, further comprising the step of:

(c) preventing use of the high-speed physical layer if the peripheral is unidentified.

8. The method of claim 4, further comprising the step of providing the identity to the peripheral through the secondary bus.

9. The method of claim 2, wherein step (b) comprises the step of using the secondary bus to detect the occurrence of a real-time connection or disconnection of a peripheral to the high-speed serial bus.

10. The method of claim 9, further comprising the step of:

(c) generating an indicator when the real-time connection or disconnection of a peripheral is detected.

11. The method of claim 10, wherein a peripheral has been connected, further comprising the steps of:

(d) accepting verification from a user of the connection of the peripheral; and

(e) permitting use of the high-speed physical layer coupling to the peripheral.

12. An apparatus for providing security from an unwanted intrusion into a system, comprising:

(a) means for coupling a host with a peripheral using a high-speed serial bus having a high-speed physical layer; and

(b) means for using features of the bus to implement the security.

13. The apparatus of claim 12, wherein means (b) uses a secondary bus within the high-speed serial bus to implement the security.

14. The apparatus of claim 13, wherein the high-speed physical layer and not the secondary bus has direct memory accessing capability.

15. The apparatus of claim 13, wherein means (b) uses the secondary bus to query an identity of the peripheral.

16. The apparatus of claim 15, further comprising:

(c) means for generating an indicator concerning the identity of the peripheral.

17. The apparatus of claim 16, further comprising:

(d) means for accepting verification from a user of the identity of the peripheral; and

(e) means for permitting use of the high-speed physical layer coupling to the peripheral.

18. The apparatus of claim 15, further comprising:

(c) means for preventing use of the high-speed physical layer if the peripheral is unidentified.

19. The apparatus of claim 15, wherein means (b) provides the identity to the peripheral through the secondary bus.

20. The apparatus of claim 13, wherein means (b) uses the secondary bus to detect the occurrence of a real-time connection or disconnection of a peripheral to the high-speed serial bus.

21. The apparatus of claim 20, further comprising:

(c) means for generating an indicator when the real-time connection or disconnection of a peripheral is detected.

22. The apparatus of claim 21, wherein a peripheral has been connected, further comprising:

(d) means for accepting verification from the user of the connection of the peripheral; and

(e) means for permitting use of the high-speed physical layer coupling to the peripheral.

23. An apparatus for providing security against unwanted access to a system having a host and a peripheral, comprising:

(a) a high-speed serial bus having a high-speed physical layer and a secondary bus for coupling the host to the peripheral, and;

(b) means for controlling the apparatus.

24. The apparatus of claim 23, wherein the means for controlling is a microprocessor on the host.

25. The apparatus of claim 23, wherein the secondary bus is used to implement the security.

26. The apparatus of claim 25, wherein the high-speed physical layer but not the secondary bus can directly access memory on the host.

27. The apparatus of claim 25, wherein the means for controlling uses the secondary bus to query an identity of the peripheral.

28. The apparatus of claim 27, wherein the means for controlling generates an indicator concerning an identity of the peripheral.

29. The apparatus of claim 28, wherein the means for controlling:
accepts verification from a user of the identity of the peripheral; and
permits use of the high-speed physical layer coupling to the peripheral.

30. The apparatus of claim 27, wherein the means for controlling prevents use of the high-speed physical layer if the peripheral is unidentified.

31. The apparatus of claim 25, wherein the means for controlling uses the secondary bus to detect the occurrence of a real-time connection or disconnection of a peripheral to the high-speed serial bus.

32. The apparatus of claim 31, wherein the means for controlling generates an indicator when the connection or disconnection of a peripheral is detected.

33. The apparatus of claim 32, wherein when a peripheral has been connected:

the means for controlling accepts verification from the user of the connection of the peripheral; and

the means for controlling permits use of the high-speed physical layer coupling to the peripheral.

34. A storage medium encoded with machine-readable computer program code for providing security from an unwanted intrusion into a system having a host computer coupled to a peripheral by a high-speed serial bus having a high-speed physical layer and a secondary bus, comprising:

(a) means for causing the host computer to supervise provision of the security; and

(b) means for causing the host computer to use features of the bus to implement the security.

35. The storage medium of claim 34, wherein means (b) comprises means for causing the host computer to use the secondary bus to implement the security.

36. The storage medium of claim 35, wherein the high-speed physical layer and not the secondary bus has direct memory accessing capability.

37. The storage medium of claim 35, wherein means (b) comprises means for causing the host computer to use the secondary bus to query an identity of the peripheral.

38. The storage medium of claim 37, further comprising:

(c) means for causing the host computer to generate an indicator concerning the identity of the peripheral.

39. The storage medium of claim 38, further comprising:

(d) means for causing the host computer to accept verification from a user of the identity of the peripheral; and

(e) means for causing the host computer to permit use of the high-speed physical layer coupling to the peripheral.

40. The storage medium of claim 37, further comprising means for causing the host computer to prevent use of the high-speed physical layer if the peripheral is unidentified.

41. The storage medium of claim 37, further comprising means for causing the host computer to provide the identity to the peripheral through the secondary bus.

42. The storage medium of claim 35, wherein means (b) comprises means for causing the host computer to use the secondary bus to detect the occurrence of a real-time connection or disconnection of a peripheral to the high-speed serial bus.

43. The storage medium of claim 42, further comprising means for causing the host computer to generate an indicator when the real-time connection or disconnection of a peripheral is detected.

44. The storage medium of claim 43, wherein a peripheral has been connected, further comprising means for causing the host computer to:

accept verification from the user of the connection of the peripheral; and

permit use of the high-speed physical layer coupling to the peripheral.

45. The storage medium of claim 34, wherein the computer program code is an operating system.

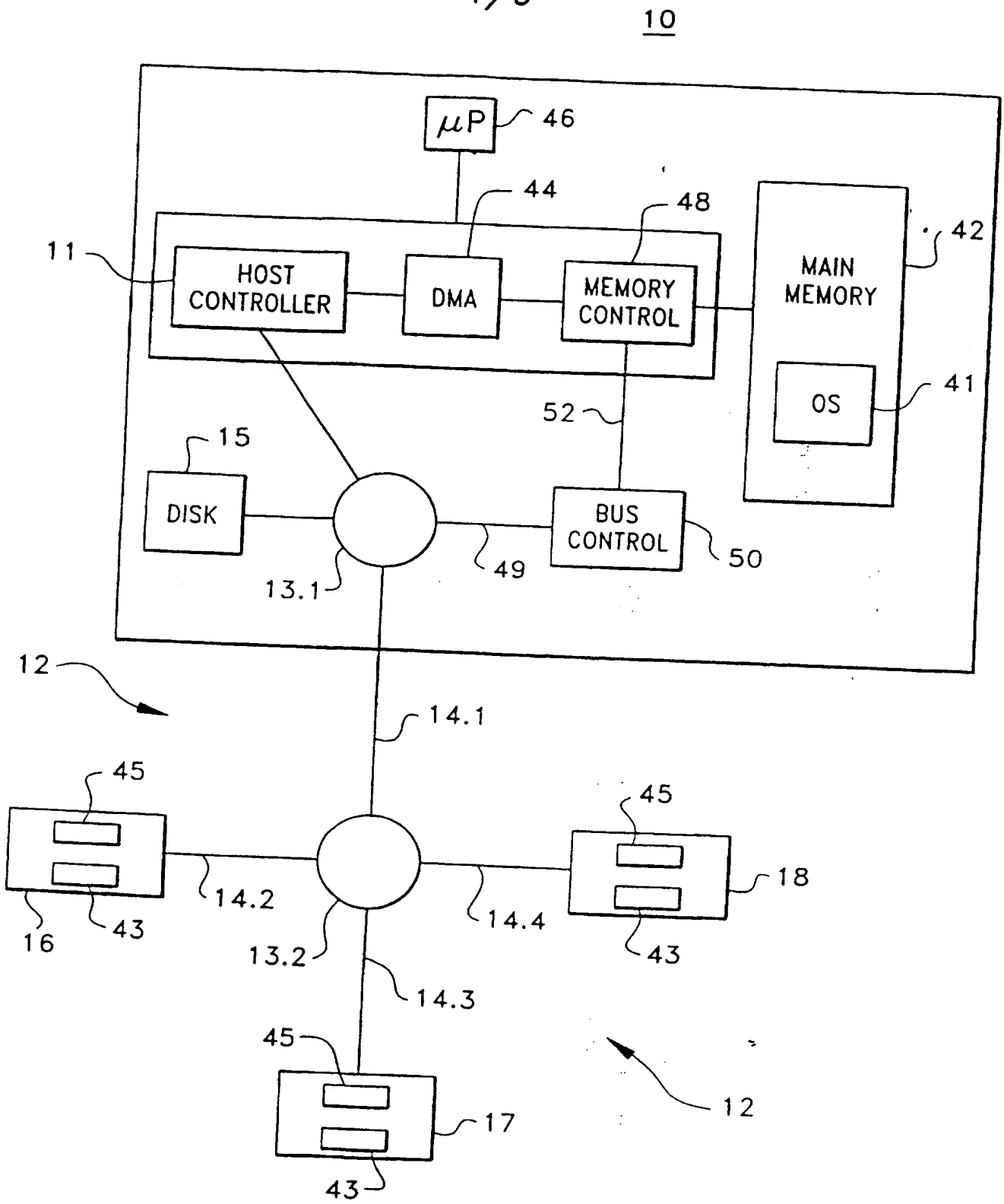

10
μP
46
44
48
42
11
HOST CONTROLLER
DMA
MEMORY CONTROL
MAIN MEMORY
OS
41
52
15
DISK
BUS CONTROL
50
49
13.1
12
14.1
45
45
18
14.2
14.4
16
43
43
13.2
14.3
45
17
43
12

FIG. 1

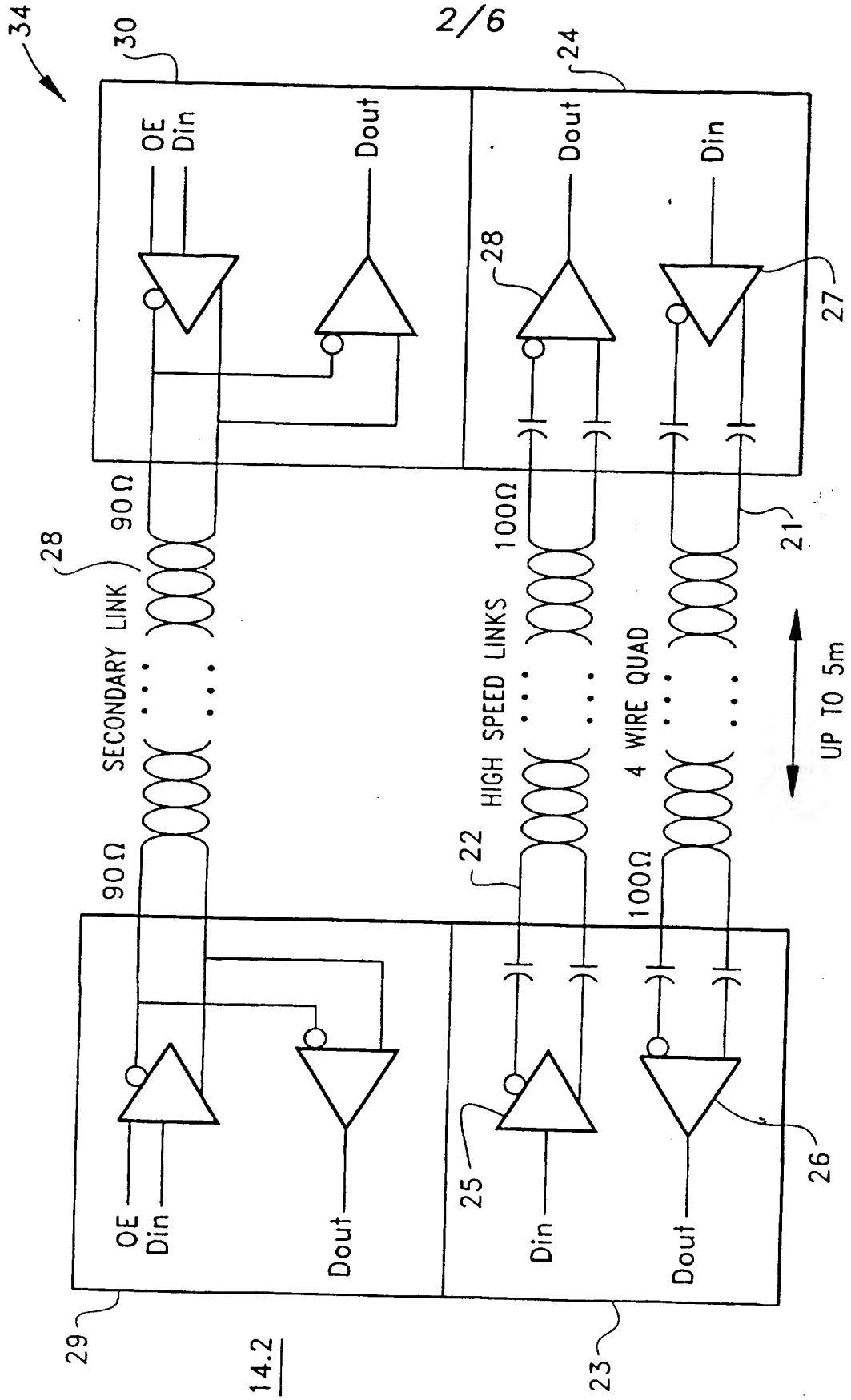

34
30
24
OE
Din
Dout
Dout
Din
28
27
90Ω
100Ω
21
28
SECONDARY LINK
HIGH SPEED LINKS
4 WIRE QUAD
UP TO 5m
90Ω
22
100Ω
OE
Din
Dout
25
Din
Dout
26
29
14.2
23

FIG. 2

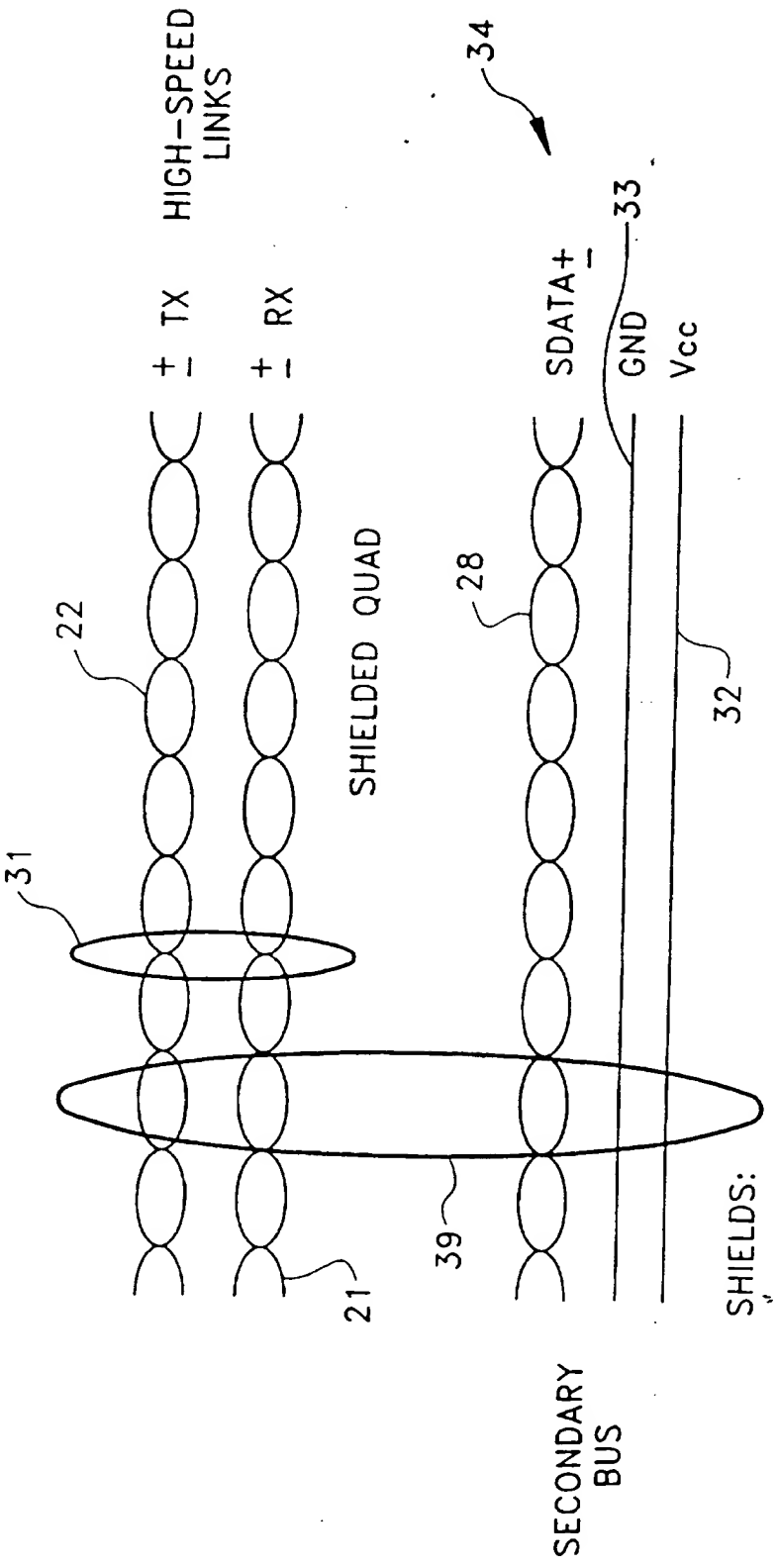

HIGH-SPEED LINKS
± TX
± RX
SHIELDED QUAD
SDATA±
GND
Vcc
SHIELDS:
SECONDARY BUS
22
31
21
39
28
32
33
34

FIG. 3

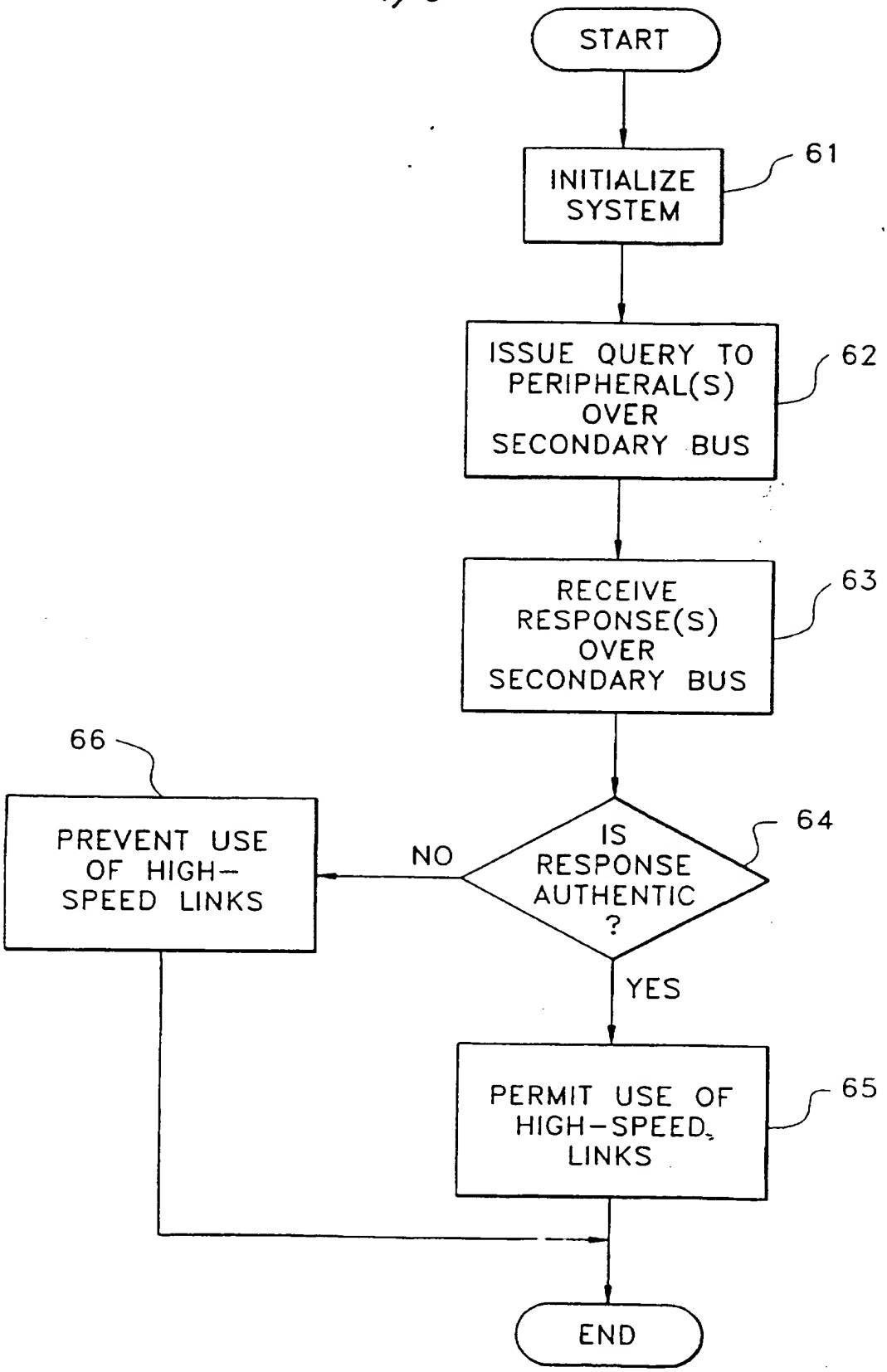

START
INITIALIZE SYSTEM
61
ISSUE QUERY TO PERIPHERAL(S) OVER SECONDARY BUS
62
RECEIVE RESPONSE(S) OVER SECONDARY BUS
63
IS RESPONSE AUTHENTIC ?
64
NO
YES
66
PREVENT USE OF HIGH-SPEED LINKS
PERMIT USE OF HIGH-SPEED LINKS
65
END

FIG. 4

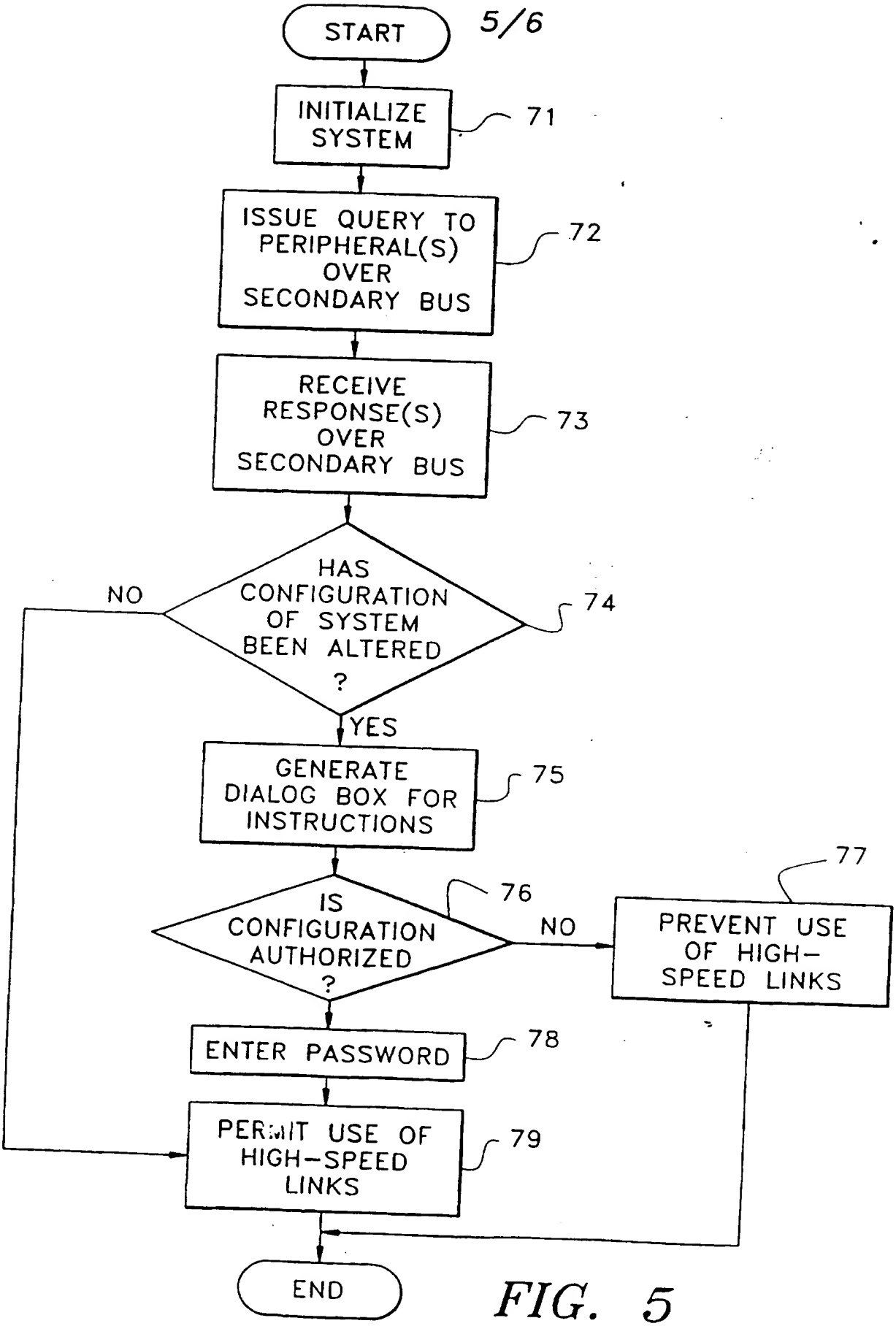

START
INITIALIZE SYSTEM
71
ISSUE QUERY TO PERIPHERAL(S) OVER SECONDARY BUS
72
RECEIVE RESPONSE(S) OVER SECONDARY BUS
73
HAS CONFIGURATION OF SYSTEM BEEN ALTERED ?
74
NO
YES
GENERATE DIALOG BOX FOR INSTRUCTIONS
75
IS CONFIGURATION AUTHORIZED ?
76
NO
77
PREVENT USE OF HIGH-SPEED LINKS
ENTER PASSWORD
78
PERMIT USE OF HIGH-SPEED LINKS
79
END

FIG. 5

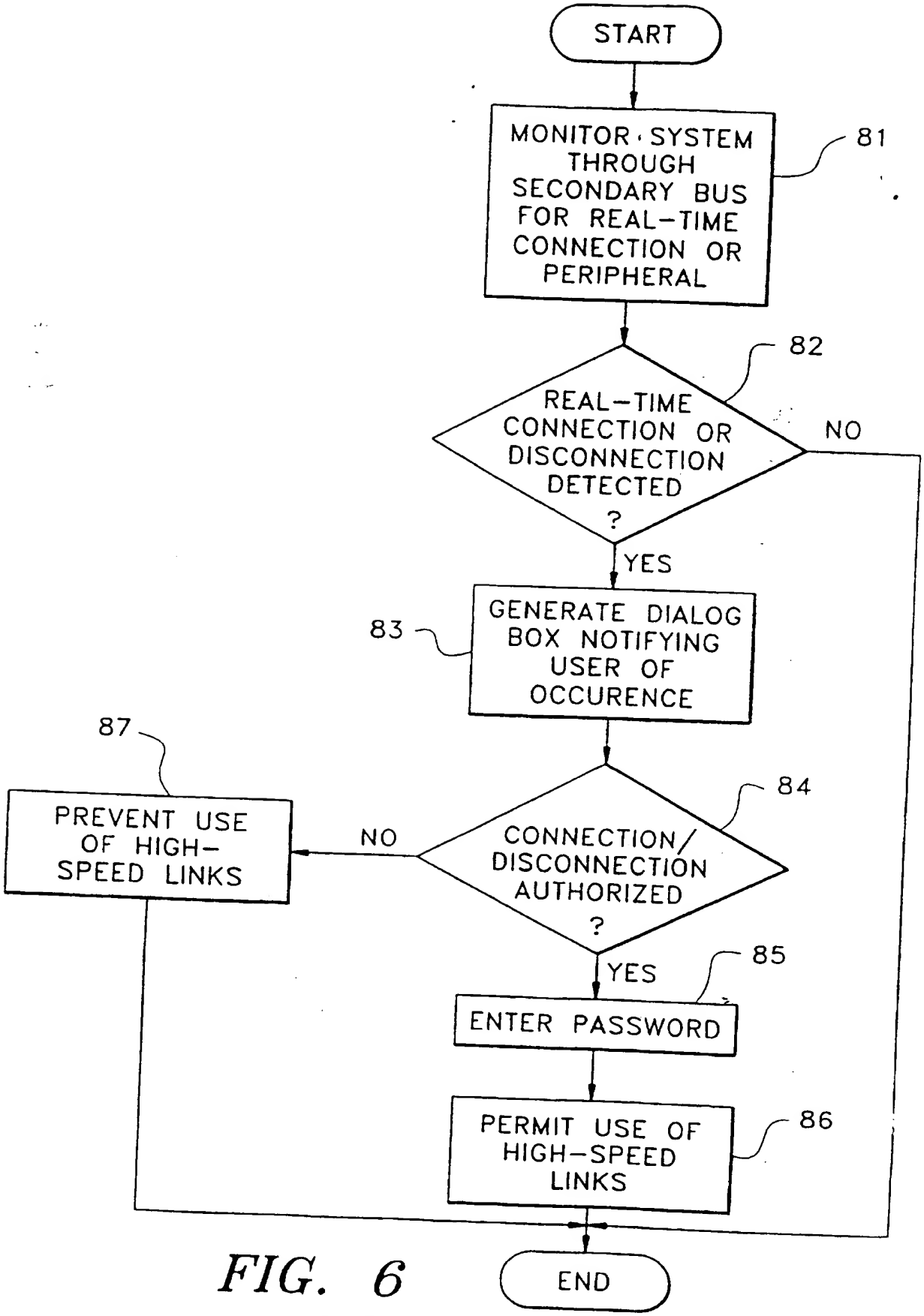

START
MONITOR SYSTEM THROUGH SECONDARY BUS FOR REAL-TIME CONNECTION OR PERIPHERAL
81
REAL-TIME CONNECTION OR DISCONNECTION DETECTED ?
82
NO
YES
GENERATE DIALOG BOX NOTIFYING USER OF OCCURENCE
83
CONNECTION/ DISCONNECTION AUTHORIZED ?
84
NO
PREVENT USE OF HIGH-SPEED LINKS
87
YES
ENTER PASSWORD
85
PERMIT USE OF HIGH-SPEED LINKS
86
END

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/04905

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 11/00
US CL : 395/186

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/186, 187.01, 188.01, 306, 307, 308, 307, 847, 828, 283, 281

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, STN, ProQuest IEEE
search terms: security, intrusion, protection, serial bus, high-speed bus, verifying, validating, checking, authorizing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,202,997 A (ARATO) 13 April 1993, col. 2, lines 31-46 and col. 3, lines 9-10, line 24 to col. 4, line 15 and col. 4, line 55, to col. 5 line 58.	1-45
Y	CLARKSON. Seriously Serial, Byte Magazine. October 1994. pages 117-122.	1-45
Y	US 5,099,417 A (MAGAR et al) 24 March 1992, Figure 1, col. 3, lines 28-51 and col. 4, line 46 to col. 5, line 61 and col. 6 lines 45-69.	3,14,26,36
Y	US 5,394,522 A (SANCHEZ-FRANK et al) 28 February 1995, col. 3, lines 39-48 and col. 5, lines 16-69.	6,11,17,22,28,29,32,33,38,39,43,44

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 JUNE 1997	26 AUG 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JOSEPH PALYS Telephone No. (703) 305-9685

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/04905

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 5,581,712 A (HERRMAN) 03 December 1996, col. 4, lines 29-33.	10,21
A	US 5,475,818 A (MOLYNEAUX et al) 12 December 1995, see entire document.	1-45
A	US 5,204,961 A (BARLOW) 20 April 1993, see entire document.	1-45
A	US 5,310,998 A (OKUNO) 10 May 1994, see entire document.	1-45
A	TEENER. A Bus on a Diet-The Serial Bus Alternative, COMPCON. IEEE. 1992. pages 316-321.	1-45